IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 6:22-cv-00127**
v.	)	
	)	
CROWDSTRIKE HOLDINGS, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC ("PacSec") files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 7,523,497 ("the '497 patent") (referred to as the "Patent-in-Suit") by Crowdstrike Holdings, Inc. ("Crowdstrike").

I. THE PARTIES

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Crowdstrike is a corporation organized under the laws of the State of Delaware with a principal office and a regular and established place of business at 206 E 9th Street Suite 1750, Austin, TX 78701. On information and belief, CROWDSTRIKE sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. CROWDSTRIKE can be served with process through their registered agent Corporation Service Company 251 Little Falls Drive, Wilmington, DE 19808 or wherever they may be found.

II. JURISDICTION AND VENUE

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to Patent, namely, 35 U.S.C. § 271.

4. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

5. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

III. INFRINGEMENT OF THE '497 PATNET

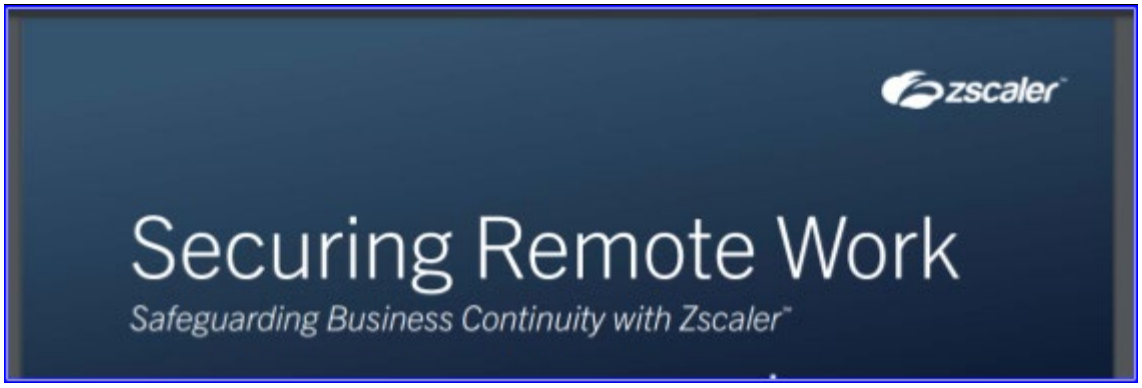
6. On April 21, 2009, U.S. Patent No. 7,523,497 ("the '497 patent", included as an attachment) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '497 patent by assignment.

7. The '497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

8. CROWDSTRIKE offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the '497 patent, including one or more of claims 1-18, literally or

under the doctrine of equivalents. Defendant put the inventions claimed by the '497 Patent into service (i.e., used them); but for Defendant's actions, the claimed-inventions embodiments involving Defendant's products and services would never have been put into service. Defendant's acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant's procurement of monetary and commercial benefit from it.

9. Support for the allegations of infringement may be found in the following preliminary table:

US7523497 B2 Claim 7	**Crowdstrike**
7. A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:	 Crowdstrike has a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets. https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/09/zScaler_Securing_Remote_Work-_Safeguarding_Business_Continuity.pdf The reference includes subject matter disclosed by the claims of the patent after the priority date. Crowdstrike was founded in 2011 and zscaler in 2007.. https://www.Crowdstrike.com/resources/datasheets/Crowdstrike_CorporateOverview_Datasheet_20200219_Web.pdf The venue of the company is: 7784+XJ Austin, Texas https://headquartersoffice.com/crowdstrike/

US7523497 B2 Claim 7	**Crowdstrike**
determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;	Zscaler's advanced security solution provides full SSL inspection and inline blocking. It provides continuous coverage for any user, anywhere, and Zscaler's advanced security solution scans every packet, every byte, every time — for both inbound and outbound traffic. It scans all communications to block botnets calling home, cookie-stealing, and anonymizers, and it provides full vulnerability-shielding. (AV-TEST GMBH provides independent third-party validation of Zscaler security protection.)[32] https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/09/zScaler_Securing_Remote_Work-_Safeguarding_Business_Continuity.pdf The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer.

US7523497 B2 Claim 7	**Crowdstrike**
classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	Zscaler's advanced security solution provides full SSL inspection and inline blocking. It provides continuous coverage for any user, anywhere, and Zscaler's advanced security solution scans every packet, every byte, every time — for both inbound and outbound traffic. It scans all communications to block botnets calling home, cookie-stealing, and anonymizers, and it provides full vulnerability-shielding. (AV-TEST GMBH provides independent third-party validation of Zscaler security protection.)[32] https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/09/zScaler_Securing_Remote_Work-_Safeguarding_Business_Continuity.pdf The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path.

US7523497 B2 Claim 7	**Crowdstrike**
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	Zscaler generates dynamic risk scores based on content and behavior, and establishes score thresholds to block zero-day threats. Zscaler has numerous industry partnerships for access to real-time intelligence feeds of known compromises, ensuring protection is updated dynamically. Every transaction is logged in detail for forensic analysis. Additionally, the Zscaler ThreatLabZ team continuously monitors online activity across more than 100 billion daily transactions to ensure that Zscaler customers are protected from the broad spectrum of known and unknown threats. (See Figure 4-18.) https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/09/zScaler_Securing_Remote_Work-_Safeguarding_Business_Continuity.pdf The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer.
US7523497 B2 Claim 7	**Crowdstrike**
allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	Zscaler generates dynamic risk scores based on content and behavior, and establishes score thresholds to block zero-day threats. Zscaler has numerous industry partnerships for access to real-time intelligence feeds of known compromises, ensuring protection is updated dynamically. Every transaction is logged in detail for forensic analysis. Additionally, the Zscaler ThreatLabZ team continuously monitors online activity across more than 100 billion daily transactions to ensure that Zscaler customers are protected from the broad spectrum of known and unknown threats. (See Figure 4-18.) https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/09/zScaler_Securing_Remote_Work-_Safeguarding_Business_Continuity.pdf The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets..

These allegations of infringement are preliminary and are therefore subject to change.

10. CROWDSTRIKE has and continues to induce infringement. CROWDSTRIKE has actively encouraged or instructed others (e.g., its customers and/or the customers of its related

companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or under the doctrine of equivalents. Moreover, CROWDSTRIKE has known of the '497 patent and the technology underlying it from at least the filing date of the lawsuit.[1] For clarity, direct infringement is previously alleged in this complaint.

11. CROWDSTRIKE has and continues to contributorily infringe. CROWDSTRIKE has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the '497 patent, literally or nder the doctrine of equivalents. Further, there are no substantial noninfringing uses for Defendant's products and services. Moreover, CROWDSTRIKE has known of the '497 patent and the technology underlying it from at least the filing date of the lawsuit. [2] For clarity, direct infringement is previously alleged in this complaint.

12. CROWDSTRIKE has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '497 patent.

IV. JURY DEMAND

PacSec3 hereby requests a trial by jury on issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, PacSec3 prays for relief as follows:

[1] Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.
[2] Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.

a. enter judgment that Defendant has infringed the claims of the '190 patent, the '564 patent and the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use DDOS protection systems;

b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patent-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;

c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;

d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;

e. declare Defendant's infringement to be willful and treble the damages, including attorneys' fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;

f. a decree addressing future infringement that either (if) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patent-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and

g. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

Ramey & Schwaller, LLP

/s/William P. Ramey
William P. Ramey, III
Texas Bar No. 24027643
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com

Attorneys for PacSec3, LLC